Security Issues in Network Virtualization for the Future Internet

Sriram Natarajan and Tilman Wolf
Department of Electrical and Computer Engineering
University of Massachusetts, Amherst, MA, USA
{snataraj,wolf}@ecs.umass.edu

***Abstract*—Network virtualization is a key technology that is necessary to support diverse protocol suites in the future Internet. A virtualized network uses a single physical infrastructure to support multiple logical networks. Each logical network can provide its users with a custom set of protocols and functionalities. Much research work has focused on developing infrastructure components that can provide some level of logical isolation between virtual networks. However, these systems often assume a somewhat cooperative environment where all network infrastructure providers, virtual network operators, and users collaborate. As this technology matures and becomes more widely deployed, it is also important to consider the effects of and possible defenses against malicious operators and users. In this paper, we explore these security issues in network virtualization. In particular, we systematically discuss the relationship between all entities and potential attacks to illustrate the importance of considering security issues in the design and implementation of virtualized networks. We also present several ideas on how to proceed toward the goal of secure network virtualization in the future Internet.**

***Index Terms*—Internet architecture, network security, network virtualization, network attacks, isolation**

I. Introduction

Future Internet architectures are currently being explored in the networking research community [1]. While the current Internet has provided a very successful communication infrastructure, there are needs for more security, support for large numbers of embedded and mobile devices, new communication paradigms, etc. For many of these new communication domains, specialized protocol suites have been developed. Due to this specialization, it is not expected that a single protocol stack can satisfy all the needs of a future Internet. Instead, it is necessary to develop a network architecture that can accommodate multiple, different protocol stacks in parallel.

Network virtualization is a potential solution that uses a single physical infrastructure that is logically shared among multiple virtual networks [2], [3]. Virtual networks can be instantiated dynamically by allocating physical resources from the physical substrate to the virtual network. These resources include link bandwidth as well as processing resources on routers in order to perform protocol processing operations. Related work has explored algorithms for mapping (i.e., resource allocation) [4] and router designs to support virtualization [5], [6].

One important aspect of network virtualization is that the three participating entities – network infrastructure providers, virtual network operators, and users – are independent and driven by different objectives. Thus, it cannot be assumed that they always cooperate to ensure all aspects of the virtual network operate correctly and securely. Instead, each entity may behave in a non-cooperative or malicious way to gain benefits. These kinds of attacks are to some extent different from what can be observed in the current Internet since they involve a different kind of underlying network architecture. We therefore believe that it is important to explore these security issues since a thorough understanding can help in developing secure network virtualization in the future Internet.

In this paper, we discuss security issues in network virtualization. In particular, we explore what potential attacks can be launched between each pair of participating entities. In this context, we discuss security requirements and attacker capabilities that underly our work. We also discuss potential defense mechanisms. While we do not discuss any specific mechanism in detail, we provide an overview that can guide future research in this domain. The specific contributions of our paper are:

- A detailed overview of security issues and vulnerabilities in the virtualized network architecture. We discuss what potential attack scenarios may arise based on the malicious actions by different entities.
- A discussion of possible defense mechanisms that can address the challenges that arise in developing secure network virtualization. We point out that basic security properties, such as confidentiality, integrity, and performance isolation can be implemented in virtual networks and thus help in achieving security.

We believe that our work points toward an interesting and important new area in network security. The remainder of this paper is organized as follows. Section II discusses the related work. Section III elaborates the network virtualization entities and Section IV discusses the security issues in network virtualization, introducing the security model and attack scenarios for each entity in the architecture. Section V discusses possible defense mechanisms and Section VI concludes the paper.

II. Related Work

The idea of network virtualization was initially proposed in the context of networking testbeds to facilitate researchers to evaluate new ideas and test experiments/protocols in realistic scenarios [7]–[10]. Virtualization in a shared testbed proved to

be successful in overcoming the limitations and complexities of individual physical testbed. To facilitate new protocol innovations in the current Internet, the idea of network virtualization has been proposed as a fundamental design principle [2], [11]. In this context, [12] proposes an architecture that separates the roles of Internet Service Providers (ISPs) into Infrastructure Providers (managing physical infrastructure) and Service Providers (running customizable network protocols and services).

Modern router designs that support network virtualization require an embedded packet processing platform that can perform custom packet processing for virtual networks that are deployed at runtime, such as [5], [13], [14]. Packet processors in these systems are often implemented using embedded multi-core network processors [15].

Security issues in virtualized network architectures impose significant challenges and requires effective solutions. The problem of hosting network protocols and services on third party infrastructures raises serious questions on the trustworthiness of the participating entities. Reference [16] shows the list of ISPs that introduce hidden traffic shaping techniques on peer-to-peer protocols. Such activities indicate the requirement to examine security issues, when hosting virtual networks on the network infrastructures. Reference [17] discusses the requirement for accountability in the hosted virtual networks. Information leakage in virtualized network infrastructures are analogous to the cloud computing paradigm. Reference [18] shows a side channel attack that extracts secret information by targeting co-hosted virtual machines using Amazon EC2 service. Reference [4] suggests a denial-of-service attack can be launched on the physical network that can bring down all hosted virtual networks. Our work, presents a systematic overview of the security concerns in virtualized networks that arise between all participating entities.

Allowing virtual networks to customize the allocated resources by introducing programmability can lead to the introduction of malicious code on the router [19]. Solutions to this problem have been proposed using techniques from embedded system security [20]. Our work does not discuss these specific issues, but looks at security issues that can also arise during normal (i.e., non-malicious) operation of virtualized networks.

III. Network Virtualization

Network virtualization enables multiple logical networks to share the physical resources of the underlying network infrastructure. This network model introduces flexibility to the Internet ossification by separating the network architecture functionalities into the following entities:

- Network Infrastructure (NI): provides the physical components required to setup the network (e.g., routers and links). NI efficiently allocates the required network bandwidth and physical resources (device CPU and memory) for each virtual network, ensuring proper resource isolation between them.
- Virtual Networks (VN): deploy customizable network protocols by leasing the required infrastructure resources from multiple NIs. Each virtual network is a combination of multiple virtual routers and links. When initiating a service, the VN confines to the Service Level Agreements (SLA) with set of NIs and receives the requested resources. Each VN then instantiates the service (e.g., novel network protocol) on the allocated resources to form a virtual network topology by connecting end users to the network.
- End Users: are similar to the current Internet architecture but have the opportunity to choose from multiple virtual network services.

For any virtual network, the above architectural separation reduces the cost involved in setting up the physical resources and maintaining them. This three-tier architecture promises to introduce flexibility through programmability, improved scalability and reduction in maintenance costs. Figure 1 shows two virtual networks sharing the network infrastructure resources. Both VNs deploy their customized network services on the shared infrastructure components and establish end-to-end connectivity between end users.

Despite the various advantages, hosting multiple virtual networks on a shared network infrastructure introduces new security challenges. The VN assumes inherent provision of security features by the hosting NI and is oblivious to the malicious activities of the infrastructure. In addition, with the infrastructure resources being shared among multiple virtual networks it presents an opportunity for attackers to co-host malicious services and attack the legitimate VNs. For the NI, the hosted virtual networks should not launch attacks or access privileged information on the infrastructure. To understand the possible security issues in detail, we focus on identifying the attacks and vulnerabilities that are unique to the virtualized network infrastructure environment.

IV. Security in Virtualized Networks

Network security is an important challenge to be addressed when adapting to new architectural innovations. The customization (programmability) functionality of the virtual networks and the provision of a shared, hosted network infrastructure introduces new security vulnerabilities. Each entity in the architecture is operated by different management units and hence we assume a mutual distrust between them. Figure 2 shows the possible combinations in which attacks can compromise different entities in the architecture. For example, (1) indicates the scenario when a malicious VN service launches attacks on the end users.

A. Virtual Networks

Virtual Networks (VN) can be targeted by attacks generated from the underlying infrastructure (NI), the co-hosted VNs or the users connected to the VN. In this section, we discuss our security model for the hosted VNs explaining the security requirements, attacker capabilities, and attack scenarios.

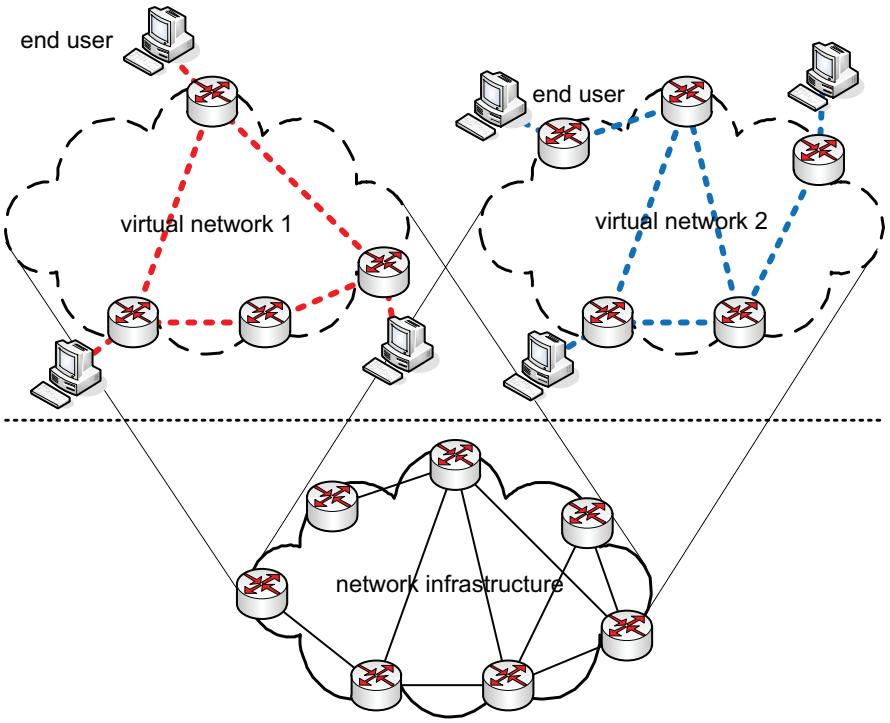

Fig. 1. Virtualized Network Infrastructure.

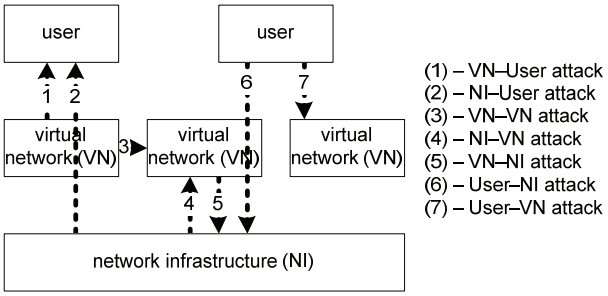

Fig. 2. Potential Attacks within Virtualized Network.

1) Security Requirements: To ensure correct protocol processing of the hosted VNs we assume the following security requirements:

- NIs should not attack or modify the working or functionality of the hosted VN.
- A co-hosted VN should not launch attacks on a vulnerable VN.
- Users should not be able to intrude and modify the functionality of the VN by taking advantage of programmability.
- An inherent access control mechanism should ensure the security of privileged information stored in VN.

2) Attacker Capabilities: The attacker capabilities that can compromise the hosted VN are:

- An attacker can instantiate a malicious protocol function to modify the normal functionality of the virtual network.
- An attacker can sniff the state of the shared physical resources on the network infrastructure to attack the co-hosted VNs.
- An attacker can intentionally modify or selectively manipulate the data traffic associated with a particular VN.

3) Attack Scenarios: Here we discuss potential vulnerabilities and attacks that can be launched on the VN by illustrating each case with an attack scenario.

a) NI attacks on VN: Network Infrastructure providers can indulge in biased management practices by introducing hidden VN monitoring activities on the network traffic, thus violating user privacy and confidentiality. To control network congestion and maintain the promised network access, the NI could introduce protocol specific interference by injecting forged packets to disrupt the legitimate connection. Recent activities by Comcast to inject RESET packets on file sharing protocol connections disrupted user activities bringing down P2P connections such as BitTorrent and Gnutella [21]. Rather than introducing dynamic traffic shaping mechanisms, the company blocked all traffic corresponding to P2P protocols by sniffing protocol headers and injecting forged packets, leading to the Net Neutrality debate [22]. Such practices exhibit the level of control the infrastructure has on the hosted virtual network, raising questions of trust and accountability.

b) VN attacks on co-hosted VN: Network virtualization projects such as [10], [12] propose that the logical isolation between the hosted virtual networks significantly improves the secureness of the system by providing better control and manageability. On the contrary the isolation of resources can lead to entirely new set of network attacks. An attacker could take advantage of the shared infrastructure platform

by leasing portion of resources to assess the vulnerabilities and functionalities of the co-hosted VNs. The vulnerable VN could be one of the competing virtual network running a specific service. Once the attacking VN is instantiated, it takes advantage of the placement and launches a cross-VN side channel attack to steal information from the vulnerable VN. An example of such an attack was exhibited in the Amazon EC2 cloud service by [18], however, we perceive similar attacks can be launched in our network virtualization scenario.

c) User attacks on VN: To reduce the complexity of network management of virtual networks, [23] suggests an interesting solution to provide a live router migration technique, transferring the control plane information (network protocol binaries and configuration files) and re-instantiating the data plane state in the new physical router platform. This approach is similar to the live virtual machine migration technique introduced in [24]. During migration of the virtual network state, an attacker sniffing the network traffic can launch a Man-in-the-Middle (migration) attack to eavesdrop the contents of the VN and other confidential information. An example of such an attack in the context of live virtual machine image migration was shown in [25].

B. Network Infrastructure

The network infrastructure is vulnerable to attacks originating from the hosted virtual networks or users associated with them. In this section, we define our security model explaining the security requirements, attacker capabilities, and attack scenarios with respect to the network infrastructure.

1) Security Requirements: For a correct functioning of the network infrastructure we assume the following security requirements:

- The hosted VN should not tamper with the allocated NI resources to gain control of the infrastructure.
- NI should ensure complete isolation of physical and network resources between co-hosted virtual networks.
- Legitimate traffic should be processed without any interference, while malicious network traffic should be inferred and discarded.
- NI should support effective access control mechanism to protect from extraction of secret information stored in the infrastructure.

2) Attacker Capabilities: The following attacker capabilities define the possible attack scenarios that can be launched on the network infrastructure:

- An attacker can send arbitrary data and control packets to flood the network and bring down the NI.
- An attacker can asses the vulnerabilities of the infrastructure from the allocated resources to intrude and take control of the entire infrastructure.
- An attacker cannot physically access the equipments but can initiate remote based attacks.

3) Attack Scenarios: The following attack scenarios exhibit the vulnerabilities in the network infrastructures:

a) User attacks on NI: Virtual network providers require flexibility in customizing their service. Modern routers use general purpose programmable packet processors that allow reprogramming the router functionality [26]. This feature however introduces new vulnerabilities threatening to compromise the entire network infrastructure. With the introduction of programmability in packet processors, code exploits such as buffer overflows, integer vulnerabilities can introduce various security issues. An attacker could inject a data packet that takes advantage of the code vulnerability of the hosted virtual network and modify the operation of the packet processor leading to a denial-of-service attack. This scenario is specific to the customization functionality introduced by the virtual network that compromises the NI. Hence a secure programming paradigm is required when instantiating the virtual network service by the network infrastructure.

b) VN attacks on NI: A malicious VN can be motivated to attack the infrastructure to disrupt the services hosted by a competing VN. The hosted platform gives extra opportunity to asses the vulnerabilities of the infrastructure and launch a flooding attack on the network and physical resources of NI that brings down the entire infrastructure, eventually breaking the co-hosted VN. Another scenario is when the attacker wishes to reproduce some hosted VN service, can manipulate the configurations of NI by extracting secret information and eavesdrop on the hosted VN traffic. An example could be a live video streaming service that can be eavesdropped, reproduced and redirected to a set of unauthorized users.

C. Users

Various network security issues and related defense mechanisms have been proposed to protect end systems. However, in this work we focus on attacks originating from a malicious virtual network or from a vulnerable network infrastructure that compromises the end user.

1) Security Requirements: The basic security requirement for end users is to ensure that attacks should not modify the working of the end-system. End users should be able to identify and discard attack traffic.

2) Attacker Capabilities: The following attacker capabilities define the possible attack scenarios that can be launched on the end users:

- An attacker can send attack packets to compromise or modify a specific functionality on the end system.
- An attacker can launch a flooding attack to send continuous network traffic and throttle the network bandwidth of the end user disrupting access to legitimate network service.
- An attacker cannot physically access the end system but can initiate remote based attacks.

3) Attack Scenarios:

a) NI attacks on User: A compromised network infrastructure can selectively drop/modify packets belonging to particular sender or group of senders. The attacker could choose to drop a packet within a particular time window, thereby forcing the sender to reduce their sending rate as

they perceive congestion. The attacker could selectively drop queued packets exploiting congestion control protocol at the senders. The VN and the sender are completely unaware of the malicious activity of the NI and hence are subjected to reduced quality of service provision.

b) VN attacks on User: A VN exploiter with malicious intent can intentionally sniff or monitor the end user network traffic. This monitoring could impose more financial constraints on the end users by raising false alarms, increasing extra financial charges. This provides an opportunity for the virtual network to advertise additive services by promising better quality with increased cost.

V. Toward Secure Network Virtualization

In this section, we discuss the challenges and required defense mechanisms to provide a secure virtualized network infrastructure platform.

A. Challenges

Virtual networks introduce unique challenges when compared with the traditional networking requirements.

- Efficient Packet Processing: An efficient packet processing methodology should be identified with certain level of data transparency between the hosted VNs and the NIs. Our attack scenarios indicate that the underlying infrastructure can introduce biased management practices, monitor confidential information, or launch hidden attacks. Hence the problem of identifying a mechanism to securely process the packets without exposing the input data is required.
- Global Connectivity: To setup end to end network connectivity, the virtual network service should partner with multiple infrastructure providers with varying levels of agreements and requirements. This requires that the virtual network should trust multiple competing network infrastructures to establish global connectivity.
- Forwarding Rate: High data rate forwarding requirements in the routers imposes significant challenge when extra processing is introduced by the security mechanisms. Most services require certain level of Quality of Service such as low latency with reliable packet processing. To meet such demands, the computation complexity introduced by the proposed security mechanisms should ensure that the forwarding data rate is not compromised.

To address the above challenges, a secure system should provide the following fundamental principles: Confidentiality, Integrity and Resource Isolation (Availability) of information. In this section we discuss possible defense mechanisms that can answer some of the important security issues, ensuring a secure hosting of virtual networks on the network infrastructures.

B. Defense Mechanism: Confidentiality

The mutual distrust between the participating entities in the network virtualization architecture raises the question of confidentially and privacy of the processed data. Considering the possible vulnerabilities as discussed in Section IV, the VN does not want to expose the data packet (header and payload) when processed by the NI. Encryption techniques are effective to ensure the confidentiality of the data traffic when processed by third party network infrastructures.

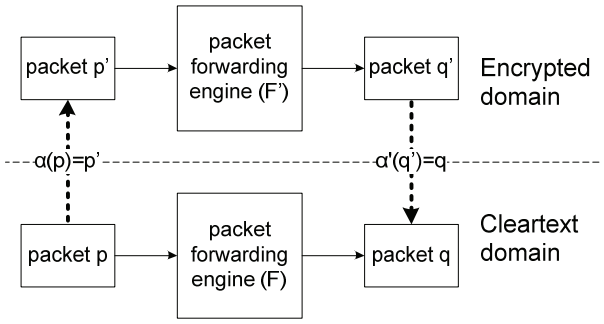

Fig. 3. Encrypted Protocol Processing.

Figure 3 shows the packet forwarding function performed in the encrypted domain. In the general case, given an input packet p, the packet forwarding engine F determines the outgoing link and sends the packet q through the appropriate interface. Since the network infrastructure is not trusted, the virtual network does not want to reveal the data packet p and hence encrypts the entire packet (header and payload data) using the encryption function $\alpha(p)$. The transformed input p' is then processed by the packet forwarding engine F' without knowing the actual content p to generate the encrypted version (q') of the output packet q. The decryption function $\alpha'(p)$ decrypts packet q' to send the output packet q. The encrypted protocol processing can reduce various security concerns for the virtual network without revealing the underlying processed data. However, the important challenge is to identify a mechanism that can support the processing of input data in the encrypted domain. Specifically, the processing technique should include the following features:

- An efficient encryption process that encrypts all incoming data with low latency requirements.
- An encrypted processing function that supports all processing features required by the hosted virtual networks.

The following defense mechanisms propose possible solutions to ensures data confidentiality and privacy. Secure tunneling protocol techniques provide the required confidentiality of the data by encapsulating the packet payload. Message Stream Encryption (MSE) protocol obfuscates the header and payload data to ensure the provision of confidentiality and authentication. To avoid biased management practices by ISPs, BitTorrent protocol versions introduced MSE based protocol encryption that enhances privacy and confidentiality [27]. However, [28] shows various potential vulnerabilities that can compromise the working of the MSE protocol. Hence, an efficient protocol processing solution that satisfies the requirements of the virtual networks and resistant to attacks is required.

Recently, Fully Homomorphic Encryption (FHE) (supports

both addition and multiplication) has theoretically proved to process the data in the encrypted domain without decrypting the input data [29]. All processing functions are performed in the encrypted domain and hence the infrastructure is completely oblivious to the data being processed. However, the practical feasibility of the FHE technique to satisfy protocol processing requirements and challenges are unclear.

C. Defense Mechanism: Integrity

Data integrity protects the information from being transformed/modified without appropriate authorization. From our attack scenarios, it is evident that both the virtual networks and network infrastructures are prone to hidden malicious attacks. The following defense mechanisms propose possible solution that ensures data integrity.

1) Trust and Accountability: Trusted computing ensures consistency in expected behaviors between participating entities. [30] proposes a trust management framework that gathers feedback from past experiences of hosting virtual network services and measures the degree of involvement in terms of nodes and links. [17] proposes to modify the network interface cards to support better detection capabilities using processor extensions and shows inherent assurance of a trusted, accountable platform. Considering the attack space discussed in Section IV, the above solutions lack the dynamics to adapt and protect from attacks. Ideally a monitoring scheme that dynamically tracks the working of the entities in runtime is suitable to ensure effective information integrity provision.

2) Monitoring: To identify the biased monitoring practices introduced by ISPs, [31] uses causal inference techniques by passively collecting performance data from clients. To isolate malicious routers, [32] uses a distributed detection technique involving neighboring routers to identify the anomalous behavior of a malicious router.

NI Monitoring: Network infrastructures should allocate the requested resources and not interfere in the working of the hosted virtual networks. However, any VN irregularities that compromise the NI should be identified using monitoring techniques. A monitoring system should include: 1) a detection mechanism that identifies the malicious activity and discard them and 2) a recovery module that resets the working state of the infrastructure (packet processor) when attacked. The NI can implement a well defined hardware monitor in the packet processor that checks instruction level operations as shown in [20].

VN Monitoring: The design of a VN monitoring system should consider the challenges and requirements introduced by the virtualized network architecture. Specifically, the VN monitor should ensure: 1) protocol processing function in the infrastructure is processed as specified and 2) any manipulations/modifications of network traffic by the underlying infrastructure should be detected. Given the architectural separation of VN and NI and the associated challenges, third party based or distributed detection techniques relying on traffic traces to identify irregularities are not suitable. Traffic validation techniques using the Conservation of Flow principles can be used to detect the anomalous behavior of the NI as shown in [33]. Given a input traffic and the expected behavior of the system, the anomalous behavior is detected when the actual network traffic deviates significantly from the expected behavior.

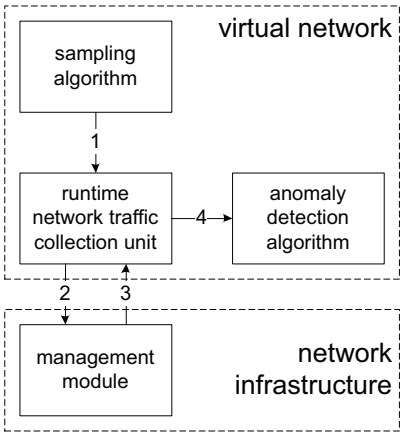

Fig. 4. Virtual Network Monitoring System.

We propose an initial design of a virtual network monitoring system. Figure 4 shows a virtual network monitoring system that evaluates the anomalous behavior of the NI. An effective sampling algorithm initiates the runtime network traffic collection unit to gather traffic statistics from the network infrastructure management module. Modern routers and switches such as [34] provides detailed network traffic statistics that can be used to detect anomalous behavior of the infrastructure. The network traffic collection unit receives the requested set of packets from the management module. The packets are then given as input to the anomaly detection algorithm. A traffic validation module in the anomaly detection algorithm then checks for the Conservation of Flow characteristics to detect any deviation from the expected behavior.

D. Defense Mechanism: Resource Isolation

Another important security concern for network virtualization is the provision of network (link bandwidth) and physical (device CPU and memory) resource isolation by the hosting network infrastructures. Isolation of network and physical resources have recently received significant attention from the research community. Slicing network bandwidth among multiple entities have well studied (VLANs and time-division multiplexing) solutions. For the physical resources, [13] proposes to use a network processor that provides the required resource isolation to the virtual network slices. [35] ensures resource isolation using a programmable logic by providing a hardware based data plane for virtualized networks. [6] proposes a network processor that introduces processor scheduling across hardware threads to ensure isolation and weighted fair access.

The above defense mechanisms are some of the fundamental requirements that can ensure secure functioning of the hosted virtual networks and the shared network infrastructure.

VI. Summary and Conclusion

Network virtualization has received significant attention in recent years. We argue that it is important to consider the security issues and vulnerabilities in the virtualized networks since their architecture is fundamentally different from the current Internet. Our work has identified potential attacks and presented some initial ideas on how to develop suitable defense mechanism. We believe that these observations provide an important first step toward a more detailed understanding of solutions to secure network virtualization in the future Internet.

Acknowledgements

This material is based upon work supported by the National Science Foundation under Grant No. 0952524.

References

[1] A. Feldmann, "Internet clean-slate design: what and why?" *SIGCOMM Computer Communication Review*, vol. 37, no. 3, pp. 59–64, Jul. 2007.

[2] T. Anderson, L. Peterson, S. Shenker, and J. Turner, "Overcoming the Internet impasse through virtualization," *Computer*, vol. 38, no. 4, pp. 34–41, Apr. 2005.

[3] J. S. Turner, "A proposed architecture for the GENI backbone platform," in *Proc. of ACM/IEEE Symposium on Architectures for Networking and Communication Systems (ANCS)*, San Jose, CA, Dec. 2006, pp. 1–10.

[4] N. M. M. K. Chowdhury and R. Boutaba, "A survey of network virtualization," *Computer Networks*, vol. 54, no. 5, pp. 862–876, Apr. 2010.

[5] M. B. Anwer, M. Motiwala, M. b. Tariq, and N. Feamster, "SwitchBlade: a platform for rapid deployment of network protocols on programmable hardware," in *Proceedings of the Conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM)*, New Delhi, India, Sep. 2010, pp. 183–194.

[6] Q. Wu, S. Shanbhag, and T. Wolf, "Fair multithreading on packet processors for scalable network virtualization," in *Proc. of ACM/IEEE Symposium on Architectures for Networking and Communication Systems (ANCS)*, San Diego, CA, Oct. 2010.

[7] *Global Environment for Network Innovation*, National Science Foundation, http://www.geni.net/.

[8] *An open platform for developing, deploying, and accessing planetary-scale services*, Planetlab Consortium, http://www.planet-lab.org/.

[9] *Network Emulation Testbed*, University of Utah, http://www.emulab.net/.

[10] A. Bavier, N. Feamster, M. Huang, L. Peterson, and J. Rexford, "In VINI veritas: realistic and controlled network experimentation," in *SIGCOMM '06: Proceedings of the 2006 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, Pisa, Italy, Aug. 2006, pp. 3–14.

[11] J. S. Turner and D. E. Taylor, "Diversifying the Internet," in *Proc. of IEEE Global Communications Conference (GLOBECOM)*, vol. 2, Saint Louis, MO, Nov. 2005.

[12] N. Feamster, L. Gao, and J. Rexford, "How to lease the Internet in your spare time," *SIGCOMM Computer Communication Review*, vol. 37, Jan. 2007.

[13] J. S. Turner, P. Crowley, J. DeHart, A. Freestone, B. Heller, F. Kuhns, S. Kumar, J. Lockwood, J. Lu, M. Wilson, C. Wiseman, and D. Zar, "Supercharging PlanetLab: a high performance, multi-application, overlay network platform," in *SIGCOMM '07: Proceedings of the 2007 conference on Applications, technologies, architectures, and protocols for computer communications*, Kyoto, Japan, Aug. 2007, pp. 85–96.

[14] D. Yin, D. Unnikrishnan, Y. Liao, L. Gao, and R. Tessier, "Customizing virtual networks with partial fpga reconfiguration," *SIGCOMM Computer Communication Review*, vol. 41, pp. 125–132, Jan. 2011.

[15] T. Wolf, "Challenges and applications for network-processor-based programmable routers," in *Proc. of IEEE Sarnoff Symposium*, Princeton, NJ, Mar. 2006.

[16] *Bad ISPs*, VUZE, http://wiki.vuze.com/w/Bad_ISPs.

[17] E. Keller, R. B. Lee, and J. Rexford, "Accountability in hosted virtual networks," in *Proc. of the First ACM SIGCOMM Workshop on Virtualized Infrastructure Systems and Architectures (VISA)*, ser. VISA '09, Barcelona, Spain, Aug. 2009, pp. 29–36.

[18] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," in *Proceedings of the 16th ACM conference on Computer and communications security*, ser. CCS '09. New York, NY, USA: ACM, 2009, pp. 199–212. [Online]. Available: http://doi.acm.org/10.1145/1653662.1653687

[19] D. Chasaki, Q. Wu, and T. Wolf, "Attacks on network infrastructure," in *Proc. of Twentieth IEEE International Conference on Computer Communications and Networks (ICCCN)*, Maui, HI, Aug. 2011.

[20] D. Chasaki and T. Wolf, "Design of a secure packet processor," in *Proc. of ACM/IEEE Symposium on Architectures for Networking and Communication Systems (ANCS)*, San Diego, CA, Oct. 2010.

[21] *FCC Rules Against Comcast for BitTorrent Blocking*, Electronic Frontier Foundation, http://www.eff.org/deeplinks/2008/08/fcc-rules-against-comcast-bit-torrent-blocking.

[22] E. Felten, *Three Flavors of Net Neutrality*, https://http://www.freedom-to-tinker.com/blog/felten/three-flavors-net-neutrality.

[23] Y. Wang, E. Keller, B. Biskeborn, J. van der Merwe, and J. Rexford, "Virtual routers on the move: live router migration as a network-management primitive," *SIGCOMM Comput. Commun. Rev.*, vol. 38, pp. 231–242, August 2008. [Online]. Available: http://doi.acm.org/10.1145/1402946.1402985

[24] C. Clark, K. Fraser, S. Hand, J. G. Hansen, E. Jul, C. Limpach, I. Pratt, and A. Warfield, "Live migration of virtual machines," in *Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation - Volume 2*, ser. NSDI'05. Berkeley, CA, USA: USENIX Association, 2005, pp. 273–286. [Online]. Available: http://portal.acm.org/citation.cfm?id=1251203.1251223

[25] J. Oberheide, E. Cooke, and F. Jahanian, "Exploiting Live Virtual Machine Migration," in *BlackHat DC Briefings*, Washington DC, February 2008.

[26] W. Eatherton, "The push of network processing to the top of the pyramid," in *Keynote Presentation at ACM/IEEE Symposium on Architectures for Networking and Communication Systems (ANCS)*, Princeton, NJ, Oct. 2005.

[27] *Message Stream Encryption*, VUZE, http://wiki.vuze.com/w/Message_Stream_Encryption.

[28] B. B. Brumley and J. Valkonen, "Attacks on message stream encryption," in *Proceedings of the 13th Nordic Workshop on Secure IT Systems—NordSec '08*, H. R. Nielson and C. W. Probst, Eds., October 2008, pp. 163–173.

[29] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the 41st annual ACM symposium on Theory of computing*, ser. STOC '09. New York, NY, USA: ACM, 2009, pp. 169–178. [Online]. Available: http://doi.acm.org/10.1145/1536414.1536440

[30] L. Mekouar, Y. Iraqi, and R. Boutaba, "Incorporating trust in network virtualization," in *Proceedings of the 2010 10th IEEE International Conference on Computer and Information Technology*, ser. CIT '10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 942–947. [Online]. Available: http://dx.doi.org/10.1109/CIT.2010.174

[31] M. B. Tariq, M. Motiwala, N. Feamster, and M. Ammar, "Detecting network neutrality violations with causal inference," in *Proceedings of the 5th international conference on Emerging networking experiments and technologies*, ser. CoNEXT '09. New York, NY, USA: ACM, 2009, pp. 289–300. [Online]. Available: http://doi.acm.org/10.1145/1658939.1658972

[32] A. T. Mizrak, Y.-C. Cheng, K. Marzullo, and S. Savage, "Detecting and isolating malicious routers," *IEEE Transactions on Dependable and Secure Computing*, vol. 3, no. 3, pp. 230–244, Jul-Sep 2006.

[33] J. Hughes, T. Aura, and M. Bishop, "Using conservation of flow as a security mechanism in network protocols," in *Security and Privacy, 2000. S P 2000. Proceedings. 2000 IEEE Symposium on*, 2000, pp. 132 –141.

[34] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: enabling innovation in campus networks," *SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69–74, Apr. 2008.

[35] M. B. Anwer and N. Feamster, "Building a fast, virtualized data plane with programmable hardware," in *Proc. of the First ACM SIGCOMM Workshop on Virtualized Infrastructure Systems and Architectures (VISA)*, Barcelona, Spain, Aug. 2009, pp. 1–8.